Utah Bureau of Criminal Identification
N E W S L E T T E R
Department of Public Safety

IDENTITY THEFT FILE

Is your agency making entries into the NCIC Identity Theft File?

Do your officers know how to respond when they get a "hit" on the file?

The NCIC Identity Theft file has been established to protect victims of identity theft, and to protect them when they come in contact with law enforcement. It also helps to identify the offenders when they come in contact with law enforcement.

If the victim of identity theft contacts your agency about the theft, please do all you can to protect the victim and apprehend the offender. Make sure you enter the **victim's** identifying information in the Identity Theft file (EID transaction.) At this point the victim needs to choose a password that you enter into the password field. The victim needs to ensure he remembers the password upon any future encounters with law enforcement.

If law enforcement runs the victim's information on NCIC in the future, an NCIC Identity Theft Hit will come back. Your officers must know how to react when they get a hit on this file! The most important thing to remember is that getting a hit on this file is not necessarily cause for arrest!

A caveat at the top of the hit says: "Warning - The identity of the subject identified in this record has been reported stolen. Review the victim profile and use caution in verifying the identity of this person. The password included in this response has been assigned to the identity theft victim. Verify that the subject of inquiry can confirm the password."

The password chosen by the victim can be found in the PWD field on the hit. If the person in custody knows the password and matches the victim description and knows the password, you are probably dealing with the victim. If the person in custody doesn't match the victim description, and does not know the password, you may be dealing with the offender!

As further protection for the victim, BCI strongly suggests attaching the victim's photo and/or fingerprint to the entry.

For further information, please see the NCIC Inquiry Power Point Presentation on the TAC web site (http://dpsemployees.utah.gov/TAC/TACHome.html) This presentation contains an example of what a "hit" on this file looks like, and where the password can be found.

OTHER STATES AND YQs

Most of you have probably noticed that not all states always follow NCIC or Nlets policy when responding to a Hit Confirmation. Unfortunately BCI has no power over how other states handle such situations.

To reduce liability, make sure YOUR agency follows all Hit Confirmation procedures. Send YQ messages according to established time frames, and also respond to YQ messages with YR responses. Don't rely on phone responses!

You get a hit on a wanted person entry from the Gooberville PD in East Dakota. You send them a YQ. Instead of sending you a YR response, they call you and say they will extradite the person. Two days later, however, they claim they never said they would extradite. The wanted person now wants to sue you for unlawful detention.

If your agency has maintained your YQ message(s) and other documentation about the hit, you will be able to back up your case. There will also be no record in NCIC's database that the Gooberville PD ever sent a YR message to you. The liability is now with Gooberville!

BCI REPRESENTATIVES

Don't forget to try and contact your designated BCI representative when you have a question or problem. This will allow your representative to become more familiar with your agency's unique problems and situations. (This also means you won't have to explain the same thing over and over to everyone at BCI!)

With only a few exceptions, representatives are over all agencies in a county, regardless of the type of agency. (Police department, court, prosecutor, etc.)

The regions are:

Davis, Weber, Morgan Counties: Mary Ann
801-965-4812

Salt Lake and Rich Counties: Adrienne
801-965-4497

Southeast (east of I-15): Marcus
801-965-4409

Southwest (west of I-15): Holly
801-964-4566

For routine situations, such as forgotten passwords, please call the 24-hour help desk at 801-965-4446.

TAC WEB SITE LOCATION

Hopefully you have all noticed the new location for the TAC web site. (Which is not just for TACs anymore!)

The site is now located at
http://dpsemployees.utah.gov/TAC/TACHome.html

Our public web site also has a new URL at http://publicsafety.utah.gov/bci/ Please refer the public to this site if they have questions about expungements, concealed weapon permits, etc.

COMMONLY MISSED TEST QUESTIONS

We noticed that some of the TAC test questions gave many of you some problems! Here are a few of the commonly missed questions and their answers:

Q. If another agency (dispatch center, etc.) actually uses a computer to make an NCIC entry for you, who is responsible for the quality and content of the information? (Introduction)

A. Your agency. Don't forget that the agency whose ORI appears on the NCIC entry is responsible for the quality and content of the information, regardless of what agency actually made the entry.

Q. An NCIC vehicle inquiry by plate number could bring back a hit on:

A. A stolen vehicle, a missing person, and/or an individual in the VGTOF file. Vehicle information can be attached to most person entries, so you never know what kind of response you will get when you run a plate number or a VIN.

Q. You need to run an NCIC inquiry on Bob Loblaw, but you have no numeric identifiers for him. Can you get any NCIC information on Bob?

A. Yes - request an "Off-Line Search" from the FBI. Agencies are always welcome to contact the FBI at 304-625-3000 whenever they do not have enough information to make an on-line search, or when an on-line search does not provide adequate results.

NEW HOURS

Don't forget that BCI is participating in the "Working 4 Utah" program, and most of our office hours have changed to 7 am to 6 pm, Monday through Thursday. The sections affected by this change are AFIS, Records, the Front Desk staff, Concealed Firearms, and Field Services.

Our Brady Bill staff and the Help Desk will continue working their normal hours. Don't forget that you can *always* call our Help Desk at 801-965-4446!

STOLEN DRIVER LICENSES

Did you know you can enter stolen driver licenses into the NCIC Article File? Did you know you can inquire on a driver license using the Article File?

When entering a driver license use IDRIVER as the TYP code. Use the OLN number as the SER number. Enter the driver license state in the BRA field. Additional information, such as the class or driver name may be entered in the MIS field.

If you believe you are dealing with a stolen license, inquire into the Article File using IDRIVER in the TYP field and the OLN in the Serial Number field.

If the owner of the driver license is also the victim of identity theft, make sure you enter the owner's information into the Identity Theft File!

MISSING PERSONS

STANDARDS FOR CALL TAKERS – MISSING CHILDREN

Reports of missing and/or sexually exploited children may be among the most difficult, challenging, and emotionally charged cases your agency will ever experience. The attitude and approach taken when responding to reports of missing and/or sexually exploited children may determine whether the child is recovered promptly and safely or remains missing in an exploitive environment. Often the initial call forms the foundation and direction of the response to that missing and/or sexually exploited child.

In an effort to develop best-practice guidelines for handling calls pertaining to missing and/or sexually exploited children, a joint steering committee on Call Center Best Practices in Cases of Missing and Sexually Exploited Children was developed. Members of the committee include the Association of Public-Safety Communications Officials (APCO), National Academies of Emergency Dispatch (NAED), National AMBER Alert Initiative (U.S. Department of Justice's Office of Justice Programs and Fox Valley Technical College), National Center for Missing & Exploited Children (NCMEC), and National Emergency Number Association (NENA). These best-practice guidelines can be found at the URL below.

http://www.apco911.org/new/commcenter911/APCOstandards.php

ADDING VEHICLE INFO TO PERSON ENTRIES

Summary from the Sacramento Bee, July 27, 2008

Georgetown resident Patricia Presba, 46, and another local man, Jaime Ramos, 21, have been arrested in Salt Lake City as suspects in the murder of her husband, Ronald Presba, El Dorado County [California] sheriff's investigators have announced.

The arrests came about a month after Ronald Presba's torched Chevrolet Suburban was found at the bottom of a ravine. Human remains were found in the vehicle but they have not yet been positively identified.

Detectives traveled to Utah to talk to Presba and Ramos after they were found in a local motel Friday. She had been reported missing from her Georgetown home Thursday under troubling circumstances - blood was found on the door and inside the home, officials said.

Presba and Ramos were arrested after the El Dorado County sheriff's detectives finished their interviews. The two suspects are expected to be extradited to El Dorado County within 15 days. Patricia Presba was apprehended Friday at a Utah motel by Salt Lake City police.

A Utah Motor Vehicle Enforcement Division officer, who was looking for stolen vehicles in the parking lot of a Salt Lake City Motel 6, came across a California plate. When the officer ran the plate number, it registered a National Crime Information Center hit to a missing person.

The officer contacted authorities in California and was told the person was wanted in connection with a possible homicide case, police said.

The officer apprehended Presba and a man when they emerged from their motel room and headed for the car.

(As mentioned on Page 2 on the commonly missed test questions – you never know what you will get when you make a vehicle inquiry!)

VICAP

ViCAP GOES ONLINE

And Closer to Investigators Who Need It

08/04/08

Since 1985, our Violent Criminal Apprehension Program, or ViCAP, has linked an untold number of seemingly unrelated violent crime investigations…and helped state and local law enforcement solve many of those cases.

Now, it's about to get even better. ViCAP will soon be available—from any Internet terminal—to participating law enforcement agencies at the local, state, and federal level.

First, a little history. ViCAP's original concept—to share investigative data from violent crimes—actually came from a local police officer. Eventually, it was decided that the FBI would house this data, primarily because of our experience in being a national repository of other types of criminal justice data, like fingerprints.

ViCAP's initial focus was transient/serial killers who crossed jurisdictional boundaries with impunity. But it expanded and now includes actual/attempted homicides, missing persons (believed victims of foul play), kidnappings (including child abductions), sexual assaults, and unidentified human remains. The database houses modus operandi, signature aspects, crime scene descriptions/photos, victim and suspect details, and other pertinent information.

ViCAP today. Our database contains about 150,000 open and closed violent crime investigations submitted by some 3,800 state and local law enforcement agencies—and includes some "cold cases" that go back to the 1950s.

Once cases are added, they are continually compared against other cases housed in the database. Based on common traits and similar modus operandi, cases that are *possibly* related are linked. Then our ViCAP analysts take over and give the process the human touch—looking for patterns to pinpoint crimes that may have been committed by the same offender, and hopefully generating new investigative leads.

ViCAP also offers additional assistance to our partners—including multi-agency coordination efforts, investigative support, case management help, crime mapping, case series matrices, and on-scene case assistance.

Evolving ViCAP access. Back in 1985, ViCAP information sat on a mainframe computer in Quantico, Virginia, accessible only to FBI personnel. Users usually submitted their case information to us through the mail.

In the mid-1990s, we migrated ViCAP to a client-server system to get the information closer to the people who needed it most—state and local law enforcement. That basically meant we put ViCAP software on desktop computers in police agencies around the country. Users were then able to electronically send us their case information, as well as any requests for assistance.

The process was faster, but we continued looking for ways to enhance it. Thus, after several years in development—and in coordination with the ViCAP advisory board of state and local representatives—ViCAP Web was born, accessible through the secure Law Enforcement Online portal.

Benefits of a web-enabled ViCAP? Formerly, only ViCAP personnel had access to the system's data. Now, agencies will have direct access to the national database so they will be able to input and retrieve data instantly, search the database for similar cases, review historical cases, and update their own investigative data. As a result, the database will be more current.

Other benefits include the ability to offer nationwide web-based training to users, faster updates and enhancements to the system, and the end of maintaining hundreds of standalone ViCAP computers.

In the short-term, law enforcement agencies will reap the benefits of this new and improved ViCAP. In the long-term, it's the American public—kept safer from violent criminals—who will benefit.

From www.fbi.gov, August 8, 2008